-2-

IN THE CLAIMS:

Amended claims follow:

1. (currently amended) A program stored on a computer-readable medium for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers, said computer program product comprising:

receiving code for receiving at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger [pattern]; and

action performing code, responsive to detection of one of said at least one predetermined trigger [pattern] to perform at least one predetermined anti-malware action.

2. (previously presented) A program stored on a computer-readable medium as claimed in claim 1, wherein said plurality of network connected computers each have a malware scanner for scanning computer files to detect malware within said computer files.

-3-

3. (previously presented) A program stored on a computer-readable medium as claimed in claim 2, wherein said malware scanner includes malware definition data for identifying malware to be detected.

4. (previously presented) A program stored on a computer-readable medium as claimed in claim 3, wherein said at least one predetermined anti-malware action includes forcing an update of malware definition data being used by one or more of said plurality of network connected computers.

5. (previously presented) A program stored on a computer-readable medium as claimed in claim 2, wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one of said malware scanners such that said at least one of said malware scanners performs more thorough malware scanning.

6. (previously presented) A program stored on a computer-readable medium as claimed in claim 1, wherein said at least one predetermined anti-malware action includes isolating at least one of said network connected computers from other parts of said computer network.

7. (previously presented) A program stored on a computer-readable medium as claimed in claim 1, wherein said managing computer stores said plurality of log data messages within a database.

-4-

8. (previously presented) A program stored on a computer-readable medium as claimed in claim 7, wherein said detecting code is operable to query said database.

9. (previously presented) A program stored on a computer-readable medium as claimed in claim 7, wherein said database includes data identifying at least one of:

malware protection mechanisms used by respective network connected computers;

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

security settings of malware protection mechanisms used by respective network connected computers.

10. (currently amended) A method of managing malware protection within a computer network containing a plurality of network connected computers, said method comprising the steps of:

receiving at a managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said

-5-

plurality of network connected computers matching at least one predetermined trigger [pattern]; and

in response to detection of said at least one predetermined trigger [pattern], performing at least one predetermined anti-malware action.

11. (original) A method as claimed in claim 10, wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files.

12. (original) A method as claimed in claim 11, wherein said malware scanner uses malware definition data to identify malware to be detected.

13. (previously presented) A method as claimed in claim 12, wherein said at least one predetermined anti-malware action includes forcing an update of malware definition data being used by at least one of said plurality of network connected computers.

14. (previously presented) A method as claimed in claim 11, wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning.

-6-

15. (previously presented) A method as claimed in claim 10, wherein said at least one predetermined anti-malware action includes isolating at least one of said network connected computers from other parts of said computer network.

16. (original) A method as claimed in claim 10, wherein said managing computer stores said plurality of log data messages within a database.

17. (previously presented) A method as claimed in claim 16, wherein said detecting step includes querying said database.

18. (previously presented) A method as claimed in claim 16, wherein said database includes data identifying at least one of:

malware protection mechanisms used by respective network connected computers;

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

security settings of malware protection mechanisms used by respective network connected computers.

-7-

19. (currently amended) Apparatus for managing malware protection within a computer network said computer network containing a plurality of network connected computers, said apparatus comprising:

receiving logic for receiving at a managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting logic for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger [pattern]; and

action performing logic, in response to detection of at least one predetermined trigger [pattern], for performing at least one predetermined anti-malware action.

20. (previously presented) Apparatus as claimed in claim 19, wherein each of said plurality of network connected computers have a malware scanner that serves to scan computer files to detected malware within said computer files.

21. (previously presented) Apparatus as claimed in claim 20, wherein said malware scanner includes malware definition data to identify malware to be detected.

22. (previously presented) Apparatus as claimed in claim 21, wherein said at least one predetermined anti-malware action includes forcing an update of malware definition data in at least one of said plurality of network connected computers.

-8-

23. (previously presented) Apparatus as claimed in claim 20, wherein said at least one predetermined anti-malware action includes altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning.

24. (previously presented) Apparatus as claimed in claim 19, wherein said at least one predetermined anti-malware action includes isolating at least one of said network connected computers from other parts of said computer network.

25. (original) Apparatus as claimed in claim 19, wherein said managing computer stores said plurality of log data messages within a database.

26. (original) Apparatus as claimed in claim 25, wherein said detecting logic is operable to query said database.

27. (previously presented) Apparatus as claimed in claim 25, wherein said database includes data identifying at least one of:

malware protection mechanisms used by respective network connected computers;

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

security settings of malware protection mechanisms used by respective network connected computers.